FortiOS - Release Notes

Version 6.4.9

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

May 10, 2022
FortiOS 6.4.9 Release Notes
01-649-764531-20220510

TABLE OF CONTENTS

Change Log

Date	Change Description
2022-04-26	Initial release.
2022-05-04	Updated Fortinet Security Fabric upgrade on page 20 and Product integration and support on page 27.
2022-05-10	Updated New features or enhancements on page 16, Resolved issues on page 31, Known issues on page 50, and Built-in IPS engine on page 62.

Introduction and supported models

This guide provides release information for FortiOS 6.4.9 build 1966.

For FortiOS documentation, see the Fortinet Document Library.

Supported models

FortiOS 6.4.9 supports the following models.

FortiGate	FG-40F, FG-40F-3G4G, FG-60E, FG-60E-DSL, FG-60E-DSLJ, FG-60E-POE, FG-60F, FG-61E, FG-61F, FG-80E, FG-80E-POE, FG-80F, FG-80F-BP, FG-80F-POE, FG-81E, FG-81E-POE, FG-81F, FG-81F-POE, FG-90E, FG-91E, FG-100E, FG-100EF, FG-100F, FG-101E, FG-101F, FG-140E, FG-140E-POE, FG-200E, FG-200F, FG-201E, FG-201F, FG-300D, FG-300E, FG-301E, FG-400D, FG-400E, FG-400E-BP, FG-401E, FG-500D, FG-500E, FG-501E, FG-600D, FG-600E, FG-601E, FG-800D, FG-900D, FG-1000D, FG-1100E, FG-1101E, FG-1200D, FG-1500D, FG-1500DT, FG-1800F, FG-1801F, FG-2000E, FG-2200E, FG-2201E, FG-2500E, FG-2600F, FG-2601F, FG-3000D, FG-3100D, FG-3200D, FG-3300E, FG-3301E, FG-3400E, FG-3401E, FG-3600E, FG-3601E, FG-3700D, FG-3800D, FG-3810D, FG-3815D, FG-5001D, FG-3960E, FG-3980E, FG-4200F, FG-4201F, FG-4400F, FG-4401F, FG-5001E, FG-5001E1
FortiWiFi	FWF-40F, FWF-40F-3G4G, FWF-60E, FWF-60E-DSL, FWF-60E-DSLJ, FWF-60F, FWF-61E, FWF-61F, FWF-80F-2R, FWF-81F-2R, FWF-81F-2R-POE, FWF-81F-2R-3G4G-POE
FortiGate Rugged	FGR-60F, FGR-60F-3G4G
FortiGate VM	FG-SVM, FG-VM64, FG-VM64-ALI, FG-VM64-ALIONDEMAND, FG-VM64-AWS, FG-VM64-AZURE, FG-VM64-GCP, FG-VM64-GCPONDEMAND, FG-VM64-HV, FG-VM64-IBM, FG-VM64-KVM, FG-VM64-OPC, FG-VM64-RAXONDEMAND, FG-VMX, FG-VM64-XEN
FortiFirewall	FFW-3980E, FFW-VM64, FFW-VM64-KVM
Pay-as-you-go images	FOS-VM64, FOS-VM64-HV, FOS-VM64-KVM, FOS-VM64-XEN

Special notices

CAPWAP traffic offloading

CAPWAP traffic will not offload if the ingress and egress traffic ports are on different NP6 chips. It will only offload if both ingress and egress ports belong to the same NP6 chip. The following models are affected:

- FG-900D
- FG-1000D
- FG-2000E
- FG-2500E

FortiClient (Mac OS X) SSL VPN requirements

When using SSL VPN on Mac OS X 10.8, you must enable SSLv3 in FortiOS.

Use of dedicated management interfaces (*mgmt1* and *mgmt2*)

For optimum stability, use management ports (*mgmt1* and *mgmt2*) for management traffic only. Do not use management ports for general user traffic.

Tags option removed from GUI

The Tags option is removed from the GUI. This includes the following:

- The *System* > *Tags* page is removed.
- The *Tags* section is removed from all pages that had a *Tags* section.
- The *Tags* column is removed from all column selections.

System Advanced menu removal (combined with System Settings)

Bug ID	Description
584254	• Removed *System* > *Advanced* menu (moved most features to *System* > *Settings* page). • Moved configuration script upload feature to top menu > *Configuration* > *Scripts* page. • Removed GUI support for auto-script configuration (the feature is still supported in the CLI). • Converted all compliance tests to security rating tests.

PCI passthrough ports

Bug ID	Description
605103	PCI passthrough ports order might be changed after upgrading. This does not affect VMXNET3 and SR-IOV ports because SR-IOV ports are in MAC order by default.

FG-80E-POE and FG-81E-POE PoE controller firmware update

FortiOS 6.4.0 has resolved bug 570575 to fix a FortiGate failing to provide power to ports. The PoE hardware controller, however, may require an update that must be performed using the CLI. Upon successful execution of this command, the PoE hardware controller firmware is updated to the latest version 2.18:

```
diagnose poe upgrade-firmware
```

AWS-On-Demand image

Bug ID	Description
589605	Starting from FortiOS 6.4.0, the FG-VM64-AWSONDEMAND image is no longer provided. Both AWS PAYG and AWS BYOL models will share the same FG-VM64-AWS image for upgrading and new deployments. Remember to back up your configuration before upgrading.

Azure-On-Demand image

Bug ID	Description
657690	Starting from FortiOS 6.4.3, the FG-VM64-AZUREONDEMAND image is no longer provided. Both Azure PAYG and Azure BYOL models will share the same FG-VM64-AZURE image for upgrading and new deployments. Remember to back up your configuration before upgrading.

FortiClient EMS Cloud registration

FortiOS 6.4.3 adds full support for FortiClient EMS Cloud service. Users will be able to register and use the service in mid-December 2020.

SSL traffic over TLS 1.0 will not be checked and will be bypassed by default

FortiOS 6.2.6 and 6.4.3 ended support for TLS 1.0 when `strong-crypto` is enabled under `system global`. With this change, SSL traffic over TLS 1.0 will not be checked so it will be bypassed by default.

To examine and/or block TLS 1.0 traffic, an administrator can either:

- Disable `strong-crypto` under `config system global`. This applies to FortiOS 6.2.6 and 6.4.3, or later versions.
- Under `config firewall ssl-ssh-profile`:
  - in FortiOS 6.2.6 and later, set `unsupported-ssl` to `block`.
  - in FortiOS 6.4.3 and later, set `unsupported-ssl-negotiation` to `block`.

Policy routing enhancements in the reply direction

When reply traffic enters the FortiGate, and a policy route or SD-WAN rule is configured, the egress interface is chosen as follows.

With `auxiliary-session enabled` in `config system settings`:

- Starting in 6.4.0, the reply traffic will not match any policy routes or SD-WAN rules to determine the egress interface and next hop.
- Prior to this change, the reply traffic will match policy routes or SD-WAN rules in order to determine the egress interface and next hop.

With `auxiliary-session disabled` in `config system settings`:

- The reply traffic will egress on the original incoming interface.

RDP and VNC clipboard toolbox in SSL VPN web mode

Press `F8` to access the RDP/VNC clipboard toolbox. The functionality in previous versions with the clipboard toolbox in the right-hand side of the RDP/VNC page has been removed in FortiOS 6.4.7.

Support for FortiGates with NP7 processors and hyperscale firewall features

FortiOS 6.4.9 includes main branch support for FortiGates with NP7 processors (FG-1800F, FG-1801F, FG-2600F, FG-2601F, FG-4200F, FG-4201F, FG-4400F, and FG-4201F). These FortiGates can also be licensed for hyperscale firewall features. Previous versions of FortiOS supported FortiGates with NP7 processors through special branch firmware builds.

For information about hyperscale firewall support for FortiOS 6.4.9, refer to the Hyperscale Firewall Release Notes.

CAPWAP offloading compatibility of FortiGate NP7 platforms

To work with FortiGate NP7 platforms, current FortiAP models whose names end with letter E or F should be upgraded to the following firmware versions:

- FortiAP (F models): version 6.4.7, 7.0.1, and later
- FortiAP-S and FortiAP-W2 (E models): version 6.4.7, 7.0.1, and later
- FortiAP-U (EV and F models): version 6.2.2 and later
- FortiAP-C (FAP-C24JE): version 5.4.3 and later

The CAPWAP offloading feature of FortiGate NP7 platforms is not fully compatible with FortiAP models that cannot be upgraded (as mentioned above) or legacy FortiAP models whose names end with the letters B, C, CR, or D. To work around this issue for these FortiAP models, administrators need to disable `capwap-offload` under `config system npu` and then reboot the FortiGate.

Changes in CLI

Bug ID	Description

673049	For `localid-type address`, unhide the `localid` option so users have the option to set the ID directly for IPv4 or IPv6 addresses.
	`config vpn ipsec phase1`
	`edit <name>`
	`set localid-type address`
	`set localid <string>`
	`next`
	`end`

Changes in GUI behavior

Bug ID	Description
728746	Users are now able to export the current view of the *Policy & Objects* > *Firewall Policy* page to CSV and JSON format.

Changes in default behavior

Bug ID	Description
728468	Previously, all IPs in the IP pool and VIP were considered as local IPs if `arp-reply` was enabled. Because of this, the new NAT46/64 IP pool and VIP implementation could not use the `arp-reply` option, and a special route needed to be added on neighboring devices to route traffic to the FortiGate. Now, the IP pool and VIP have been removed from the local IP list, and the `arp-reply` option can be used for NAT46/64 IP pool and VIP (special routes on other devices are no longer required). This is an optimization of the kernel processing flow, without any command line changes on the user side.

Changes in table size

Bug ID	Description
733978	Increase per-VDOM table size for DNS server (`system.dns-database`) to 4096 for all models.
749024	Increase maximum explicit proxy user limit. The new limits are as follows: • Desktop models = 1,000 • 1U models = 12,000 • 1K models = 32,000 • 2K models = 64,000 • 3K, 4K, and 6K models = 128,000

New features or enhancements

More detailed information is available in the New Features Guide.

Bug ID	Description

613092	Allow SSL VPN to be explicitly enabled or disabled from the GUI and CLI. To connect, SSL VPN must be enabled and the SSL VPN interface must be up.
	`config vpn ssl settings`
	`set status {enable | disable}`
	`end`

648609	Add HA support for multiple ACI clusters for Cisco ACI external SDN connector VMs. The multiple IPs in the Cisco ACI external SDN connector VM configuration allows the FortiGate to connect to SDN connector VMs in the same ACI cluster in a round-robin fashion. Only one SDN connector VM is active, and the remaining serve as backups if the active one fails.
	`config system sdn-connector`
	`edit "ACI-1"`
	`set type aci`
	`set server-list "10.105.152.96" "10.105.152.97" "100.101.1.98"`
	`set server-port 5671`
	`set username "admin"`
	`set password **********`
	`next`
	`edit "ACI-2"`
	`set type aci`
	`set server-list "20.105.152.91" " 20.105.152.92" "40.111.1.3"`
	`set server-port 5671`
	`set username "admin"`
	`set password **********`
	`next`
	`end`
	ACI-1 and ACI-2 are different ACI clusters. They each have multiple SDN connector VMs in synchronization. Each firewall address can point to either ACI-1 or ACI-2.

660283	Add system event logs for the execution of CLI commands. When `cli-audit-log` is enabled under `system global`, the execution of `execute`, `config`, `show`, `get`, and `diagnose` commands will trigger system event logs.

684133	Support site-to-site IPsec VPN in an asymmetric routing scenario with a loopback interface as a VPN bound interface.
	`config vpn ipsec phase1-interface`
	`edit <name>`
	`set interface "loopback"`
	`set loopback-asymroute {enable | disable}`

Bug ID	Description
	next end
688237	Add support for a FortiGate to manage a Procend 180-T DSL transceiver (FN-TRAN-DSL) that is plugged in to an SFP port. The management of the DSL transceiver includes the ability to program the physical layer attributes on the DSL module, retrieve the status and statistics from the module, support firmware upgrades of the module, and reset the module. Supported VDSL profiles: 8a, 8b, 8c, 8d, 12a, 12b, 17a, and 30a. Supported platforms: FG-80F, FG-81F, FG-80F-BP, FGR-60F, and FGR-60F-3G4G.
696412	Allow inspection of double-tagged (802.1Q + 802.1Q) traffic on virtual wire pairs with wildcard VLANs. Other enhancements include optimizing NPU receive packet steering and configuring traffic distribution on the ISF to achieve higher throughput.

707143	NetFlow and SFlow now support using SD-WAN in interface-select-method for selecting the outgoing interface.
	`config system {netflow sflow vdom-netflow vdom-sflow}`
	`set interface-select-method {auto | sdwan | specify}`
	`set interface <interface>`
	`end`

714788	Add HA uninterruptible upgrade option, which allows users to configure a timeout value in minutes (1 - 30, default = 30) where the primary HA unit waits before the secondary HA unit is considered upgraded.
	`config system ha`
	`set uninterruptible-primary-wait <integer>`
	`end`

731532	When a FortiGate is in NAT mode, a VLAN tag with a drop eligible indicator (DEI) bit set resets to 0 after passing through the FortiGate.
735938	On the *NAC Policy* configuration page, specifying FortiSwitch groups is now supported. Previously, individual FortiSwitches had to be specified. The CLI command to specify individual switches is now updated to specify switch groups.
738640	Add 100 Mbps transceiver support for FGR-60F and FGR-60F-3G4G.
740204	Supply better heartbeat timing information to the auto-scale callback URL. Previously, the auto-scale heartbeat request made to the auto-scale callback URL did not contain a timestamp or sequence number. This information was estimated in the cloud function called by the callback URL, but the cloud function platform's timing was not as reliable as initially expected.
747640	Support Q-in-Q (802.1Q in 802.1Q) for FortiGate-VMs.
756538	Add Windows 11 and macOS 12 to the SSL VPN OS check. The following options are available for `config os-check-list <name>`: `macos-bigsur-11`, `macos-catalina-10.15`, `macos-mojave-10.14`, `macos-monterey-12`, `windows-7`, `windows-8.1`, `windows-10`, and `windows-11`. Operating systems no longer supported by FortiClient were removed.

Bug ID	Description
756639	Update the OVF package so it reflects newer VMware ESXi and hardware versions.
758560	Add macOS 12 and Windows 11 to SSL VPN host check. Windows 8 and macOS 10.9 to 10.13 are removed from the SSL VPN host check.
767575	Updating dynamic addresses using the OpenStack SDN connector now supports: Rocky, Stein, Train, Ussuri, Victoria, Wallaby, and Xena.
773530	Allow a two-hour grace period for Flex-VMs to begin passing traffic upon retrieving a license from FortiCare without VM entitlement verification from FortiGuard.

Upgrade information

Supported upgrade path information is available on the Fortinet Customer Service & Support site.

To view supported upgrade path information:

1. Go to https://support.fortinet.com.
2. From the *Download* menu, select *Firmware Images*.
3. Check that *Select Product* is *FortiGate*.
4. Click the *Upgrade Path* tab and select the following:
   - *Current Product*
   - *Current FortiOS Version*
   - *Upgrade To FortiOS Version*
5. Click *Go*.

Device detection changes

In FortiOS 6.0.x, the device detection feature contains multiple sub-components, which are independent:

- Visibility – Detected information is available for topology visibility and logging.
- FortiClient endpoint compliance – Information learned from FortiClient can be used to enforce compliance of those endpoints.
- Mac-address-based device policies – Detected devices can be defined as custom devices, and then used in device-based policies.

In 6.2, these functionalities have changed:

- Visibility – Configuration of the feature remains the same as FortiOS 6.0, including FortiClient information.
- FortiClient endpoint compliance – A new fabric connector replaces this, and aligns it with all other endpoint connectors for dynamic policies. For more information, see Dynamic Policy - FortiClient EMS (Connector) in the *FortiOS 6.2.0 New Features Guide*.
- MAC-address-based policies – A new address type is introduced (MAC address range), which can be used in regular policies. The previous device policy feature can be achieved by manually defining MAC addresses, and then adding them to regular policy table in 6.2. For more information, see MAC Addressed-Based Policies in the *FortiOS 6.2.0 New Features Guide*.

If you were using device policies in 6.0.x, you will need to migrate these policies to the regular policy table manually after upgrade. After upgrading to 6.2.0:

1. Create MAC-based firewall addresses for each device.
2. Apply the addresses to regular IPv4 policy table.

In 6.4.0, device detection related GUI functionality has been relocated:

1. The device section has moved from *User & Authentication* (formerly *User & Device*) to a widget in *Dashboard*.
2. The email collection monitor page has moved from *Monitor* to a widget in *Dashboard*.

In 6.4.4, a new sub-option, *Delete*, was added when right-clicking on the device. This option is not available when the device is online, or the device is retrieved from FortiClient.

FortiClient Endpoint Telemetry license

Starting with FortiOS 6.2.0, the FortiClient Endpoint Telemetry license is deprecated. The FortiClient Compliance profile under the Security Profiles menu has been removed as has the Enforce FortiClient Compliance Check option under each interface configuration page. Endpoints running FortiClient 6.2.0 now register only with FortiClient EMS 6.2.0 and compliance is accomplished through the use of Compliance Verification Rules configured on FortiClient EMS 6.2.0 and enforced through the use of firewall policies. As a result, there are two upgrade scenarios:

- Customers using only a FortiGate device in FortiOS 6.0 to enforce compliance must install FortiClient EMS 6.2.0 and purchase a FortiClient Security Fabric Agent License for their FortiClient EMS installation.
- Customers using both a FortiGate device in FortiOS 6.0 and FortiClient EMS running 6.0 for compliance enforcement, must upgrade the FortiGate device to FortiOS 6.2.0, FortiClient to 6.2.0, and FortiClient EMS to 6.2.0.

The FortiClient 6.2.0 for MS Windows standard installer and zip package containing FortiClient.msi and language transforms and the FortiClient 6.2.0 for macOS standard installer are included with FortiClient EMS 6.2.0.

Fortinet Security Fabric upgrade

FortiOS 6.4.9 greatly increases the interoperability between other Fortinet products. This includes:

- FortiAnalyzer 6.4.8
- FortiManager 6.4.8
- FortiClient EMS 6.4.3 build 1600 or later
- FortiClient 6.4.3 build 1608 or later
- FortiAP 6.4.4 build 0456 or later
- FortiSwitch 6.4.5 build 0461 or later

When upgrading your Security Fabric, devices that manage other devices should be upgraded first. Upgrade the firmware of each device in the following order. This maintains network connectivity without the need to use manual steps.

1. FortiAnalyzer
2. FortiManager
3. Managed FortiExtender devices
4. FortiGate devices
5. Managed FortiSwitch devices
6. Managed FortiAP devices
7. FortiClient EMS
8. FortiClient
9. FortiSandbox
10. FortiMail
11. FortiWeb
12. FortiADC

13. FortiDDOS
14. FortiWLC
15. FortiNAC
16. FortiVoice

If Security Fabric is enabled, then all FortiGate devices must be upgraded to 6.4.9. When Security Fabric is enabled in FortiOS 6.4.9, all FortiGate devices must be running FortiOS 6.4.9.

Minimum version of TLS services automatically changed

For improved security, FortiOS 6.4.9 uses the `ssl-min-proto-version` option (under `config system global`) to control the minimum SSL protocol version used in communication between FortiGate and third-party SSL and TLS services.

When you upgrade to FortiOS 6.4.9 and later, the default `ssl-min-proto-version` option is TLS v1.2. The following SSL and TLS services inherit global settings to use TLS v1.2 as the default. You can override these settings.

- Email server (`config system email-server`)
- Certificate (`config vpn certificate setting`)
- FortiSandbox (`config system fortisandbox`)
- FortiGuard (`config log fortiguard setting`)
- FortiAnalyzer (`config log fortianalyzer setting`)
- LDAP server (`config user ldap`)
- POP3 server (`config user pop3`)

Downgrading to previous firmware versions

Downgrading to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account
- session helpers
- system access profiles

Amazon AWS enhanced networking compatibility issue

With this enhancement, there is a compatibility issue with 5.6.2 and older AWS VM versions. After downgrading a 6.4.9 image to a 5.6.2 or older version, network connectivity is lost. Since AWS does not provide console access, you cannot recover the downgraded image.

When downgrading from 6.4.9 to 5.6.2 or older versions, running the enhanced NIC driver is not allowed. The following AWS instances are affected:

C5	Inf1	P3	T3a
C5d	m4.16xlarge	R4	u-6tb1.metal
C5n	M5	R5	u-9tb1.metal
F1	M5a	R5a	u-12tb1.metal
G3	M5ad	R5ad	u-18tb1.metal
G4	M5d	R5d	u-24tb1.metal
H1	M5dn	R5dn	X1
I3	M5n	R5n	X1e
I3en	P2	T3	z1d

A workaround is to stop the instance, change the type to a non-ENA driver NIC type, and continue with downgrading.

FortiLink access-profile setting

The new FortiLink `local-access` profile controls access to the physical interface of a FortiSwitch that is managed by FortiGate.

After upgrading FortiGate to 6.4.9, the interface `allowaccess` configuration on all managed FortiSwitches are overwritten by the default FortiGate `local-access` profile. You must manually add your protocols to the `local-access` profile after upgrading to 6.4.9.

To configure `local-access` profile:

```
config switch-controller security-policy local-access
    edit [Policy Name]
        set mgmt-allowaccess https ping ssh
        set internal-allowaccess https ping ssh
    next
end
```

To apply `local-access` profile to managed FortiSwitch:

```
config switch-controller managed-switch
    edit [FortiSwitch Serial Number]
        set switch-profile [Policy Name]
        set access-profile [Policy Name]
    next
end
```

FortiGate VM with V-license

This version allows FortiGate VM with V-License to enable `split-vdom`.

To enable `split-vdom`:

```
config system global
   set vdom-mode [no-vdom | split vdom]
end
```

FortiGate VM firmware

Fortinet provides FortiGate VM firmware images for the following virtual environments:

Citrix Hypervisor 8.1 Express Edition

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.OpenXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the QCOW2 file for Open Source XenServer.
- `.out.CitrixXen.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains the Citrix XenServer Virtual Appliance (XVA), Virtual Hard Disk (VHD), and OVF files.

Linux KVM

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.kvm.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains QCOW2 that can be used by `qemu`.

Microsoft Hyper-V Server 2019 and Windows Server 2012R2 with Hyper-V role

- `.out`: Download the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.out.hyperv.zip`: Download the 64-bit package for a new FortiGate VM installation. This package contains three folders that can be imported by Hyper-V Manager. It also contains the file `fortios.vhd` in the Virtual Hard Disks folder that can be manually added to the Hyper-V Manager.

VMware ESX and ESXi

- `.out`: Download either the 64-bit firmware image to upgrade your existing FortiGate VM installation.
- `.ovf.zip`: Download either the 64-bit package for a new FortiGate VM installation. This package contains Open Virtualization Format (OVF) files for VMware and two Virtual Machine Disk Format (VMDK) files used by the OVF file during deployment.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal, https://support.fortinet.com. After logging in select *Download* > *Firmware Image Checksums*, enter the image file name including the extension, and select *Get Checksum Code*.

FortiGuard update-server-location setting

The FortiGuard `update-server-location` default setting is different between hardware platforms and VMs. On hardware platforms, the default is `any`. On VMs, the default is `usa`.

On VMs, after upgrading from 5.6.3 or earlier to 5.6.4 or later (including 6.0.0 or later), `update-server-location` is set to `usa`.

If necessary, set `update-server-location` to use the nearest or low-latency FDS servers.

To set FortiGuard `update-server-location`:

```
config system fortiguard
   set update-server-location [usa|any]
end
```

FortiView widgets

Monitor widgets can be saved as standalone dashboards.

There are two types of default dashboard settings:

- Optimal: Default dashboard settings in 6.4.1
- Comprehensive: Default Monitor and FortiView settings before 6.4.1

Filtering facets are available for FortiView widgets in full screen and standalone mode.

WanOpt configuration changes in 6.4.0

Port configuration is now done in the profile protocol options. HTTPS configurations need to have certificate inspection configured in the firewall policy.

In FortiOS 6.4.0, `set ssl-ssh-profile certificate-inspection` must be added in the firewall policy:

```
config firewall policy
    edit 1
        select srcintf FGT_A:NET_CLIENT
        select dstintf FGT_A:WAN
        select srcaddr all
        select dstaddr all
```

```
        set action accept
        set schedule always
        select service ALL
        set inspection-mode proxy
        set ssl-ssh-profile certificate-inspection
        set wanopt enable
        set wanopt-detection off
        set wanopt-profile "http"
        set wanopt-peer FGT_D:HOSTID
    next
end
```

WanOpt and web cache statistics

The statistics for WanOpt and web cache have moved from *Monitor* to a widget in *Dashboard*.

IPsec interface MTU value

IPsec interfaces may calculate a different MTU value after upgrading from 6.2.

This change might cause an OSPF neighbor to not be established after upgrading. The workaround is to set `mtu-ignore` to `enable` on the OSPF interface's configuration:

```
config router ospf
    config ospf-interface
        edit "ipsce-vpnx"
            set mtu-ignore enable
        next
    end
end
```

HA role wording changes

The term master has changed to primary, and slave has changed to secondary. This change applies to all HA-related CLI commands and output. The one exception is any output related to VRRP, which remains unchanged.

Virtual WAN link member lost

The member of `virtual-wan-link` is lost after upgrade if the `mgmt` interface is set to `dedicated-to management` and part of an SD-WAN configuration before upgrade.

Enabling match-vip in firewall policies

As of FortiOS 6.4.3, `match-vip` is not allowed in firewall policies when the action is set to accept.

Hardware switch members configurable under system interface list

Starting in FortiOS 6.4.7, hardware switch members are also shown under `config system interface` with limited configuration options available.

Product integration and support

The following table lists FortiOS 6.4.9 product integration and support information:

Web Browsers	• Microsoft Edge • Mozilla Firefox version 99 • Google Chrome version 100 Other web browsers may function correctly, but are not supported by Fortinet.
Explicit Web Proxy Browser	• Microsoft Edge • Mozilla Firefox version 74 • Google Chrome version 80 Other web browsers may function correctly, but are not supported by Fortinet.
FortiManager	See important compatibility information in Fortinet Security Fabric upgrade on page 20. For the latest information, see FortiManager compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiManager before upgrading FortiGate.
FortiAnalyzer	See important compatibility information in Fortinet Security Fabric upgrade on page 20. For the latest information, see FortiAnalyzer compatibility with FortiOS in the Fortinet Document Library. Upgrade FortiAnalyzer before upgrading FortiGate.
FortiClient: • **Microsoft Windows** • **Mac OS X** • **Linux**	• 6.4.0 See important compatibility information in FortiClient Endpoint Telemetry license on page 20 and Fortinet Security Fabric upgrade on page 20. FortiClient for Linux is supported on Ubuntu 16.04 and later, Red Hat 7.4 and later, and CentOS 7.4 and later. If you are using FortiClient only for IPsec VPN or SSL VPN, FortiClient version 6.0 and later are supported.
FortiClient iOS	• 6.4.0 and later
FortiClient Android and FortiClient VPN Android	• 6.4.0 and later
FortiClient EMS	• 6.4.0
FortiAP	• 5.4.2 and later • 5.6.0 and later
FortiAP-S	• 5.4.3 and later • 5.6.0 and later
FortiAP-U	• 5.4.5 and later
FortiAP-W2	• 5.6.0 and later

FortiSwitch OS (FortiLink support)	• 3.6.9 and later
FortiController	• 5.2.5 and later Supported models: FCTL-5103B, FCTL-5903C, FCTL-5913C
FortiSandbox	• 2.3.3 and later
Fortinet Single Sign-On (FSSO)	• 5.0 build 0306 and later (needed for FSSO agent support OU in group filters) • Windows Server 2019 Standard • Windows Server 2019 Datacenter • Windows Server 2019 Core • Windows Server 2016 Datacenter • Windows Server 2016 Standard • Windows Server 2016 Core • Windows Server 2012 Standard • Windows Server 2012 R2 Standard • Windows Server 2012 Core • Windows Server 2008 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package) • Windows Server 2008 Core (requires Microsoft SHA2 support package) • Novell eDirectory 8.8
FortiExtender	• 4.0.0 and later. For compatibility with latest features, use latest 4.2 version.
AV Engine	• 6.00170
IPS Engine	• 6.00122
Virtualization Environments	
Citrix	• Hypervisor 8.1 Express Edition, Dec 17, 2019
Linux KVM	• Ubuntu 18.0.4 LTS, 4.15.0-72-generic, QEMU emulator version 2.11.1 (Debian 1:2.11+dfsg-1ubuntu7.21)
Microsoft	• Windows Server 2012R2 with Hyper-V role • Windows Hyper-V Server 2019
Open Source	• XenServer version 3.4.3 • XenServer version 4.1 and later
VMware	• ESX versions 4.0 and 4.1 • ESXi versions 4.0, 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, and 7.0

Language support

The following table lists language support information.

Language support

Language	GUI
English	✓
Chinese (Simplified)	✓
Chinese (Traditional)	✓
French	✓
Japanese	✓
Korean	✓
Portuguese (Brazil)	✓
Spanish	✓

SSL VPN support

SSL VPN web mode

The following table lists the operating systems and web browsers supported by SSL VPN web mode.

Supported operating systems and web browsers

Operating System	Web Browser
Microsoft Windows 7 SP1 (32-bit & 64-bit)	Mozilla Firefox version 99 Google Chrome version 100
Microsoft Windows 10 (64-bit)	Microsoft Edge Mozilla Firefox version 99 Google Chrome version 100
Ubuntu 20.04 (64-bit)	Mozilla Firefox version 99 Google Chrome version 100
macOS Monterey 12.3	Apple Safari version 15 Mozilla Firefox version 99 Google Chrome version 100
iOS	Apple Safari

Operating System	Web Browser
	Mozilla Firefox Google Chrome
Android	Mozilla Firefox Google Chrome

Other operating systems and web browsers may function correctly, but are not supported by Fortinet.

Resolved issues

The following issues have been fixed in version 6.4.9. For inquires about a particular bug, please contact Customer Service & Support.

Anti Spam

Bug ID	Description
743693	Anti spam engine crashes when extracting a malformed IP address from Received: headers.

Anti Virus

Bug ID	Description
665173	Crash logs are sometimes truncated/incomplete.

Application Control

Bug ID	Description
752569	Per IP shaper under application list does not work as expected for some applications.

Data Leak Prevention

Bug ID	Description
745369	PDF corruption over HTTP by DLP.

DNS Filter

Bug ID	Description
748227	DNS proxy generated local out rating (FortiGuard category) queries can time out if they are triggered for the same DNS domains with the same source DNS ID.
751759	DNS filter breaks DNS zone transfer because the client socket might close prematurely (in which there is still some data in the user space) if the server side closed the connection.

Endpoint Control

Bug ID	Description
666426	IPsec VPN does not have FCT client IP to send to EMS if using DHCP-over-IPsec.
693010	No FortiClient entry in `diagnose endpoint record list` when the FortiClient is registered on EMS with a WiFi tunnel mode interface.
738614	EMS Cloud does not update the IP for dynamic address on the FortiGate.
743235	Dynamic group EMS tags are not showing up for connected wireless devices.
744613	EMS endpoint IP and MAC addresses are not synchronized to the ZTNA tags on the FortiGate.

Explicit Proxy

Bug ID	Description
607230	Percent encoding is not converted in FTP over HTTP explicit proxy.
638172	Proxy policy matching should support choosing the best internet service name when the IP matches multiple object names.
674996	WAD encounters segmentation crash at `wad_ssl_arm_close`; crash occurred on explicit web proxy.
695468	Unable to load URL when application control or AV are enabled in a proxy policy.
721039	Short disconnections of streaming applications (Teams and Whereby) through explicit proxy.
747840	When configuring authentication schemes to negotiate and NTLM (mix), Firefox may not show the authentication pop-up with an explicit proxy.

Bug ID	Description
754259	When an explicit proxy policy has a category address as destination address, the FortiGate needs to check if the address is a Google Translate URL for extra rating. This will trigger a keyword match. However, if a web filter profile is not set yet, WAD will crash. The fix will delay the keyword match until a web filter profile is present.
757736	HTTPS TLS 1.3 handshake fails with internal error alert.

Firewall

Bug ID	Description
729245	HTTP/1.0 health check should process the whole response when `http-match` is set.
730803	Applying a traffic shaping profile and outbound bandwidth above 200000 blocks the traffic.
738584	Firewall is using the wrong NAT IP address to send out traffic after removing the VIP and its associated policy.
743160	SYN-ACK is dropped when application control with `auto-asic-offload` and NP acceleration are enabled in a firewall policy.
744888	FortiGate drops SERVER HELLO when accessing some TLS 1.3 websites using a flow-based policy with SSL deep inspection.
745853	FortiGate stops sending logs to Netflow traffic because the Netflow session cleanup routine runs for too long when there are many long live sessions in the cache.
746891	Auto-update script sent from FortiOS GUI has a policy ID of zero, which causes FortiManager to be out of synchronization.
754240	After a session updates its shaping policy, if the new shaping policy does not configure a per-IP shaper, the session will still use the old per-IP shaper from the previous shaping policy.

FortiView

Bug ID	Description
741792	Update FortiAnalyzer license REST API to use the FortiAnalyzer's licenses when in analyzer-collector mode.

GUI

Bug ID	Description
608770	When there is no IP/IPv6 address setting for *Zone*, the GUI incorrectly displays *0.0.0.0/0.0.0.0* for *IP/Netmask* and *::/0* for *IPv6 Address*.
610572	Guest user credentials never expire if a guest user logs in via the WiFi portal while an administrator is actively viewing the user's account via the GUI. If the administrator clicks *OK* in the user edit dialog after the guest user has logged in, the user's current login session is not subject to the configured expiration time.
650327	The values for `set gui-default-policy-columns` does not work for the `srcaddr`, `dstaddr`, and `source` columns.
696573	Firewall policy not visible in the GUI when enabling `internet-service src`.
699508	When an administrator ends a session by closing the browser, the administrator timeout event is not logged until the next time the administrator logs in.
704618	When login banner is enabled, and a user is forced to re-login to the GUI (due to password enforcement or VDOM enablement), users may see a *Bad gateway error* and HTTPSD crash.
720613	The event log sometimes contains duplicated lines when downloaded from the GUI.
720657	Unable to reuse link local or multicast IPv6 addresses for multiple interfaces from the GUI.
733375	On the *VPN* > *SSL-VPN Settings* page, after clicking *Apply*, `source-address` objects become `source-address6` objects if IPv6 is enabled.
734157	On a downstream FortiGate, going to *VDOM FG-traffic* > *Network* > *Interfaces* takes a long time to load.
740254	Unable to view log details for *Oracle.GlassFish.Server.ThemeServlet.Directory.Traversal* log when clicking *Details* in the GUI.
740508	Bandwidth widget shows incorrect traffic on FG-40F.
742561	On the *Network* > *Interfaces* page, after upgrading to FortiOS 6.4.7, a previously valid VLAN switch VLAN ID of 0 now displays the error message *The minimum value is 2*.
745325	When creating a new (public or private) SDN connector, users are unable to specify an *Update interval* that contains *60*, as it will automatically switch to *Use Default*.
745998	An IPsec phase 1 interface with a name that contains a `/` cannot be deleted from the GUI. The CLI must be used.
750490	Firewall policy changes made in the GUI remove the replacement message group in that policy.

HA

Bug ID	Description
658839	Cloning a policy from the CLI causes the HA cluster to get out of sync.
680753	`admin-restrict-local` feature does not work on management interface in HA cluster.
711521	When HA failover happens, there is a time difference between the old secondary becoming new primary and the new primary's HA ID getting updated. If a session is created in between, the session gets a wrong HA ID, which indicates incorrectly that the session's traffic needs to be handled by new secondary.
714788	Uninterruptible upgrade might be broken in large scale environments.
717788	FGSP has problem at failover when NTurbo or offloading is enabled (IPv4) with virtual wire pair traffic.
725240	HA cluster goes out of sync due to mismatched `vpn.certificate.crl` checksum.
729607	FTP transfers drop in active-active mode in cases where expectation sessions accumulated in the secondary unit reach the maximum number (128).
732201	VDOM restore on an already configured VDOM causes high CPU sometimes on the primary.
740743	When enabling `lag-out-port-select`, both cluster units simultaneously reboot.
740933	HA goes out of synchronization when uploading a local certificate.
744349	Unable to connect to FortiSandbox Cloud through proxy from secondary node in an HA cluster.
744826	API key (token) on the secondary device is not synchronized to the primary when `standalone-config-sync` is enabled.
746008	DNS may not resolve on the correct blade in a 6K/7K virtual cluster environment.
747270	When the HA secondary device relays logs to the primary device, it may encounter high CPU usage.
752892	PPPoE connection gets disconnected during HA failover.
757494	Unable to add a member to an aggregate interface that is down in a HA cluster.

Intrusion Prevention

Bug ID	Description
665755	The global UTM profiles named with a `g-` prefix are shared between all VDOMs and logically do not belong to any VDOM. When they are changed, the ipshelper cannot always refresh its configuration because the ipshelper tries to check each VDOM profile.
682071	IPS signatures not working with VIP in proxy mode.

Bug ID	Description
746467	IPS engine crashes when IPS injects packets to vNP and vNP/DPDK fails to restart (crashes and sometimes is out of service).
751027	FortiGate can only collect up to 128 packets when detected by a signature.
755859	The IPS sessions count is higher than system sessions, which causes the FortiGate to enter conserve mode.

IPsec VPN

Bug ID	Description
668997	*Duplicate entry found* error shown when assigning multiple dialup IPsec tunnels with the same secondary IP in the GUI.
673049	FortiGate not sending its external interface IP in the IKE negotiation (Google Cloud Platform).
680783	Traffic is dropped in policy-based mode with FEC and NTurbo enabled.
684133	Site-to-site IPsec VPN cannot establish in asymmetric routing scenario where the IPsec VPN bound interface is a loopback interface.
691178	Exchanging IPs does not work with multiple dynamic tunnels.
691718, 728276	Traffic cannot pass through IPsec tunnel after FEC is enabled on server side if NAT is enabled between VPN peers.
696835	An iked kernel panic occurs whenever a large download is initiated over an IPsec dialup tunnel.
701404	Routes are not added or removed as expected when failover occurs with IPsec FGSP HA.
715671	Traffic is failing on dialup VPN IKEv2 with EAP authentication.
717082	FortiGate keeps initiating DHCP SA rekey after lifetime expires.
718617	In an IPsec tunnel XAuth with RADIUS, the RADIUS Accounting Stop packet is missing the Acct-Input-Octets/Acct-Output-Octets attribute.
720689	Kernel crash occurs with FEC enabled on IPsec VPN when corrupted packets are received.
725551	IKE idle timeout timers continue running when the HA state switches to secondary.
726326	IPsec server with NP offloading drops packets with an invalid SPI during rekey.
726450	Local out dialup IPsec traffic does not match policy-based routes.
729760	The ADVPN forwarder does not currently track the shortcut query that it forwards. Shortcut queries and replies are forwarded or terminated solely based on the route lookup.
735412	IKE HA resynchronizes the synchronized connection without an established IKE SA.
735430	TCP SYN-ACKs are silently dropped if the traffic is sourced from a dialup IPsec tunnel and UTM is enabled.

Bug ID	Description
740475	Traffic cannot be sent out through IPsec VPN tunnel because SA is pushed to the wrong NP6 for platforms where NP6 is standalone. Affected models: FG-2000E and FG-2500E.
743732	If a failure happens during negotiating a shortcut IPsec tunnel, the original tunnel NAT-T setting is reset by mistake.
744598	Tunnel interface MTU settings do not work when `net-device` is enabled in phase 1.
745331	IPsec server with NP offloading drops packets with an invalid SPI during rekey.
747123	In an IPsec aggregate tunnel interface where one of the members is down and has an MTU of zero, and the other tunnel is up and has a non-zero MTU, the interface will take the minimum of both MTU values, which is zero. This results in no traffic going in the outbound direction.
752947	The hub sometimes allows the IKEv2 IPsec tunnel with a spoke to be established that uses an expired or revoked certificate.
765868	The packets did not pass through QTM, and SYN packets bypass the IPsec tunnel once traffic is offloaded. Affected platforms: NP7 models.

Log & Report

Bug ID	Description
712037	FortiAnalyzer OFTP connection is re-initialized every 30 seconds when the FortiGate connects to an unauthorized FortiAnalyzer.
715549	On the *Log & Report* > *SSL* page, the *Service* for SSL logs is displayed as FTPS instead of SSL.
718140	Logs are missing on FortiGate Cloud from a certain point.
724827	Syslogd is using the wrong source IP when configured with `interface-select-method auto`.
731154	SSL VPN tunnel down event log (log ID 39948) is missing.
745310	Need to add the MIGSOCK send handler to flush the queue when the first item is added to the syslog queue to avoid logs getting stuck.
745689	Unknown interface is shown in flow-based UTM logs.
749842	The miglogd process uses high CPU when handling a web rating error log that is reported with an invalid VDOM ID.
751358	Unable to set source IP for FortiCloud unless FortiCloud is already activated.
754143	Add `srcreputation` and `dstreputation` fields in the forward traffic logs to provide the reputation level of the source and destination when the traffic matches an entry in the internet service database.

Proxy

Bug ID	Description
568905	WAD crashes due to RCX having a null value.
582464	WAD SSL crash due to wrong cipher options chosen.
712584	WAD memory leak causes device to go into conserve mode.
726999	WAD crash on `wad_hash_map_del`.
728641	SSL renegotiation fails when Firefox offers TLS 1.3, but the server decides to use TLS 1.2.
733135	Web filter is blocking websites in proxy mode due to SSL certificate validation failure, which is caused by an unreachable OCSP server.
733760	Proxy inspection firewall policy with proxy AV blocks POP3 traffic of the Windows 10 built-in Mail app.
737737	WAD crashes when firewall FQDN address is null.
739627	`diagnose wad stats policy list` does not show statistics correctly when enabling certificate inspection and HTTP policy redirect.
743746	WAD encounters signal 11 crash when adding user information.
744756	Web proxy forward server group could not recover sometimes if the FQDN is not resolved.
747250	When a timeout happens while forticron is downloading a file, the original downloaded file is not be deleted, so the next successful download has extra data in front.
752744	Proxy-based certificate with deep inspection fails upon receipt of a large handshake message.
754969	Explicit FTP proxy chooses random destination port when the FTP client initiates an FTP session without using the default port.
756394	WAD crashes due to memory corruption.
756603	WAD memory spike when downloading files larger than 4 GB.
756616	High CPU usage in proxy-based policy with deep inspection and IPS sensor.
756887	WAD crashes if the certificate authentication request context is not closed in the following scenarios: when fnbamd returns a failure certificate authentication result or no response; and when the CA certificate is updated and the certificate cache is flushed.
758086	HTTPS traffic gets SSL error when deep inspection and an AV of file filter profile are enabled.
764193	The three-way handshake packet that was marked as `TCP port number reused` cannot pass through the FortiGate, and the FortiGate replies with a `FIN, ACK` to the client.

REST API

Bug ID	Description
743169	Update various REST API endpoints to prevent information in other VDOMs from being leaked.
743743	httpsd crashes due to `GET /api/v2/log/.../virus/archive` request when the `mkey` is not provided.
768056	HTTPS daemon is not responsive when successive API calls are made to create an interface.

Routing

Bug ID	Description
670031	LDAP traffic that originates from the FortiGate is not following SD-WAN rule.
693988	For DSL interface, adding static route with `set dynamic-gateway enable` does not add route to routing table.
707143	Suggest adding an option for NetFlow to use SD-WAN.
723726	TCP session drops between virtual wire pair with `auto-asic-offload` enabled in policy.
724574, 731248	BFD neighborship is lost between hub and spoke. One side shows BFD as down, and other side does not show the neighbor in the list.
724887	`set interface-select-method` takes a long time to take effect for DNS local out traffic when the source IP is specified.
725322	Improve the help text for `distance` to indicate that 255 means unreachable.
727812	ADVPN does not work with RIP as the routing protocol when `net-device` is enabled.
729002	PIM/PIM6 does not send out unicast packet with the correct source IP if interface is not specified.
731941	`Disconnected from FortiAnalyzer` events reported when the `interface-select-method` is set to `specify`, and the `interface port_<x>` is set to an interface that does not have the highest priority in the SD-WAN interface selection.
736705	ZEBOS launcher is unable to start and crashes constantly if `aspath` has more than 80 characters in the `config router router-map > set-aspath` setting.
737898	OSPFv3 cannot install IPv6 ECMP routes when both ABR next hops are in the same subnet.
746000	Multicast streams sourced on SSL VPN client are not registered in PIM-SM.
748733	Remote IP route shows `incomplete inactive` in the routing table, which causes issues with BGP routes where the peer is the next hop.
769321	After ADVPN HA failover, BGP is not established, and tunnels are up but not passing traffic between the hub and spokes.

Security Fabric

Bug ID	Description
635183	ACI dynamic address cannot be retrieved in HA vcluster2 from SDN connector.
670451	ACI SDN connector (connected by `aci-direct`) shows `curl` error 7 when updating from second VDOM.
735717	vmwd gives an error when folders are created in the vSphere web interface, and vmwd ignores the IP addresses from vApp.
738344	When CSF root synchronizes a large automation setting (over 16000) to the downstream FortiGate, csfd crashes while trying to process the relay message.
741346	The variable `%%date%%` resolves into `1900-01-00` instead of actual date when the schedule trigger type is used.
742743	Security rating Issue with unused deny policies.
745263	*AV & IPS DB Update* automation trigger is not working when clicking *Update Licenses & Definitions Now* in the GUI.
746950	When an Azure network interface ID contains upper case letters, the Azure SDN connector may not retrieve that network interface.

SSL VPN

Bug ID	Description
586035	The policy `script-src 'self'` will block the SSL VPN proxy URL.
673320	Pop-up window does not load correctly when accessing internal application at https://re***.wo***.nl using SSL VPN web mode.
676391	`set banned-cipher` command does not work for TLS 1.3.
676673	Ciphers with ARIA, AESCCM, and CHACHA cannot be banned for SSL VPN.
677057	SSL VPN firewall policy creation via CLI does not require setting user identity.
693237	DCE/RPC sessions are randomly dropped (`no session matched`).
693519	SSL VPN authentication fails for PKI user with LDAP.
695386	SAML login failure when a user belongs to multiple groups associated with multiple VPN realms.
706646	SolarWinds Orion NPM platform's web application has issues in SSL VPN web mode.
707792	SSL VPN connection breaks when deleting irrelevant CA and PKI is involved.
711974	SSL VPN bookmarks are not working correctly with multiple SD-WAN zones.

Bug ID	Description
718133	In some conditions, the web mode JavaScript parser will encounter an infinite loop that will cause SSL VPN crashes.
718142	The map integrated in the public site is not visible when using SSL VPN web mode.
726338	The wildcard matching method does not always work as expected because the kernel sometimes does not have the address yet.
726576	Internal webpage with JavaScript is not loading in SSL VPN web mode.
729426	The wildcard FQDN does not always work reliably in cases where the kernel does not have the address yet.
731278	Customer internal website (ac***.sa***.com) does not load properly when connecting via SSL VPN web mode.
737154	Slow RDP response when using SSL VPN web mode access.
737341	Some links and buttons are not working properly when accessing them through SSL VPN web mode.
737894	If there are no users or groups in an SSL VPN policy, the SSL VPN daemon may crash when an FQDN is a destination address in the firewall policy.
738711	FortiClient error message is not pertinent when the client does not meet host checking requirements.
744494	Memory occupied by the SSLVPN daemon increase significantly while the process is busy.
744899	SSL VPN RDP bookmark is not working when using Chrome 93 32-bit. Firefox 64-bit and Chrome 64-bit are still not supported on Windows 32-bit.
745499	In cases where a user is establishing two tunnel connections, there is a chance that the second session knocks out the first session before it is updated, which causes a session leak.
746990	RADIUS accounting messages after SSL VPN do not include the Class attribute (Group name).
747352	Internal web server page, https://te***.ss***.es:10443, is not loading properly in SSL VPN web mode.
748085	Authentication request of SSL VPN realm can now only be sent to user group, local user, and remote group that is mapped to that realm in the SSL VPN settings. The authentication request will not be applied to the user group and remote group of non-realm or other realms.
748667	Remove the maximum check for resolution of RDP/VNC in web portal.
749452	SSL VPN login authentication times out if primary RADIUS server becomes unavailable.
749918	Keyboard keys do not work with RDP bookmarks when PT-BR and PT-BR-ABNT2 layouts are chosen.
752055	VNC (protocol version 3.6/3.3) connection is not working in SSL VPN web mode.
755296	SSL VPN web mode has issues accessing https://e***.or***.kr.
756561	Outdated OS support for host check should be removed.

Bug ID	Description
764853	SSL VPN bookmark of VNC is not using ZRLE compression and consumes more bandwidth to end clients.
767818	SSL VPN bookmark issues with internal website.
768994	SSL VPN crashed when closing web mode RDP after upgrading to 6.4.7.

Switch Controller

Bug ID	Description
740661	FortiGate loses FortiSwitch management access due to excessive configuration pushes.

System

Bug ID	Description
488400	FGFM sessions time out when the session between two EMAC VLANs with no VLAN IDs are offloaded.
514239	There are no kernel routing updates when the session is re-initialized at the DSLAM side. DSL creates a default route to 240.0.0.1 after changing any configuration on the DSL interface.
572038	VPN throughput dropped when FEC is enabled.
572847	The wan1, wan2, and dmz interfaces should not be configured as hardware switch members on the 60F series. The wan interface should not be configured as a hardware switch member on the 40F series.
596942	SoC3 platforms may encounter kernel panic in cases when a PKCE IOCTL wait event is interrupted by WAD diagnose CLI commands.
643558	System halts after running `execute update-now` in FIPS-CC mode.
644616	NP6 does not update session timers for traffic IPsec tunnel if established over one pure EMAC VLAN interface.
651626	A session clash is caused by the same NAT port. It happens when many sessions are created at the same time and they get the same NAT port due to the wrong port seed value.
671116	Lack of null pointer check in NP6XLite driver may lead to kernel panic. Affected models: FG-40F, FG-60F, and FG-101F.
671824	On FG-40F, get `NP6XLITE: failed to read lif accounting` message on console.
681322	TCP 8008 permitted by authd, even though the service in the policy does not include that port.

Bug ID	Description
682227	DSL creates a default route to 240.0.0.1 after changing any configuration on a DSL interface.
683929	IPv6 health check cannot send probe packets even if the IPv6 gateway is configured under `configure members` view.
686367	SFP port status is not correct under `get system interface transceiver` due to incorrect i2c reading/writing. Affected platforms: FG-110xE, FG-220xE, FG-330xE, FG-340xE, FG-360xE, and FG-390xE.
687398	Multiple SFPs and FTLX8574D3BCL in multiple FG-1100E units have been flapping intermittently with various devices.
693344	port1 physical status is down. Affected models: FG-110xE, FG-220xE, FG-330xE, FG-340xE, FG-360xE, and FG-390xE.
696556	Support `gtp-enhance-mode` (GTP-U) on FG-3815D.
699152	QinQ (802.1ad) support needed on the following models: FG-1100E, FG-1101E, FG-2200E, FG-2201E, FG-3300E, FG-3301E, FG-3600E, and FG-3601E.
702932	FG-1500D reboots suddenly after COMLog reported kernel panic and voipd is tainted.
702966	There was a memory leak in the administrator login debug that caused the getty daemon to be killed.
703131	Split-task VDOM does not update IPS/AV from ha-direct connected internal FortiManager.
703219	Kernel panic on FG-101F due to lack of null pointer check on NP6XLite driver.
704981	LLDP transmission fails if there are nested software switches.
706543	FortiGuard DDNS does not update the IP address when the PPPoE reconnects.
706588	Interoperability issue between FortiGate aggregate interface and Cisco 9K switch.
710477	Unexpected output in `get system interface transceiver`. Affected models: FG-110xE, FG-220xE, FG-330xE, FG-340xE, FG-360xE, and FG-390xE.
710958	Multiple SFP ports on Nexus 7K go into a suspended state as no LACP PDUs are received.
712258	SFP28 ports on FG-340xE/FG-360xE cannot receive or transmit packets when the speed is set to 1000full. This issue is triggered by warm rebooting the FortiGate/Cisco switch or disconnecting the fiber cable.
713835	The BLE pin hole behavior should not be applied on FG-100F generation 1 that has no BLE built in.
714805	FortiManager shows auto update for down port from FortiGate, but FortiGate event logs do not show any down port events when user shuts down the `ha monitor dev`.
715234	Packets are dropped for 30 seconds during or after massive configuration commit.
715978	NTurbo does not work with EMAC VLAN interface.
716169, 767848	SFP interface is set as `1000full` is down after rebooting.
716341	SFP28 port flapping when the speed is set to 10G.

Bug ID	Description
716483	DNS proxy is case sensitive when resolving FQDN, which may cause DNS failure in cases where local DNS forwarder is configured.
718571	In cases where there are a lot of DHCP relay interfaces (such as 1000) and an interface is added or deleted, DHCP relay takes a long time to release and initialize all interfaces before it works again.
721487	FortiGate often enters conserve mode due to high memory usage by httpsd process.
721789	Account profile settings changed after firmware upgrade.
722547	Fragmented SKB size occurs if the tail room is too small to carry the NTurbo `vtag`, which causes packets to be dropped.
722781	MAC address flapping on the switch is caused by a connected FortiGate where IPS is enabled in transparent mode.
724065	`Power supply 2 DC is lost` log only appears when unplugging the power cable from power supply 2.
724779	HPE setting of NTurbo host queue is missing and causes IPS traffic to stop when HPE is enabled.
725264	FG-600E copper speed LED does not work.
726634	NTP daemon is not responding when using the manual setting.
727343	Quarantined IP is not synchronized in FortiController mode.
727829	DNS FQDN was not synchronized amongst all the working blade, so each blade might have different IP from the same FQDN. If policy a uses the FQDN as the address, it will cause the IP address of FQDN to not be in the list for the current blade, so the traffic will not match this FQDN policy.
728647	DHCP discovery dropped on virtual wire pair when UTM is enabled.
729939	Multiple processes crashing at the same time causes the device's management functionality to be unavailable when the packet size is smaller than `FSAE_HEADER_SIZE(6)`.
732633	DNS query timeout log generated for first entry in DNS domain list when multiple domains are added.
732760	SNMP trap packets are sometimes not sent from the primary `ha-direct` interface to all SNMP managers after upgrading.
738332	Connectivity issue with FortiGuard after upgrading from 7.0.0 to 7.0.1 when `ha-direct` is enabled.
738640	Add support for FS-TRAN-FX 100 Mbps SFP optical transceivers on the FGR-60F and FGR-60F-3G4G models. Previously, there was no I2C reading/writing handler in drivers for FGR-60F and FGR-60F-3G4G.
740649	FortiGate sends CSR configuration without double quote (") to FortiManager.
741944	The forticron process has a memory leak if there are duplicated entries in the external IP range file.
742471	Parsing FFDB may cause a crash when loading at reboot if the versions of FFDB_APP and FFDB_GEO_ID_FILE are different.

Bug ID	Description
743431	DDNS hostname is not correct when two VDOMs are configured.
744892	DNS query responses can be bumped when dealing with a high volume of visibility hostname log requests.
745017	`get system checksum status` should only display checksums for VDOMs the current user has permissions for.
747508	Default FortiLink configuration on FG-81F running versions 6.4.6 to 6.4.8 does not work as expected.
747834	Unexpected behavior of SNMP fgLogDeviceCachedCount value for syslog.
748409	Client traffic from VLAN to VXLAN encapsulation traffic is failing after upgrading from 6.2.7 to 6.4.6.
749835	Traffic logs reports ICMP destination as unreachable for received traffic
751523	When changing mode from DHCP to static, the existing DHCP IP is kept so no CLI command is generated and sent to FortiManager.
753602	FG-40F has a newcli signal 11 crash.
754567	FortiGate receives `Firmware image without valid RSA signature loaded` error when loading the image from FortiCloud.
754951	Static ARP entry was removed while using DHCP relay.
755746	SoC3 platforms failed to boot up when upgrading from 6.2.10 or 6.4.8.
755953	Direct CLI script from FortiManager fails due to additional `end` at the end of `diagnose debug crashlog read`.
756139	When split port is enabled on four 10 GB ports, only one LACP port is up, and the other ports do not send/receive the LACP PDU.
756445	Flow-based inspection on WCCP (L2 forwarding) enabled policy with VLAN interfaces causes traffic to drop if `asic-offload` is enabled.
756713	Packet Loss on the LAG interface (eight ports) in static mode. Affected models: FG-110xE, FG-220xE, and FG-330xE.
756779	NP7 platforms will very sparsely stop forwarding traffic with the root cause at QTM.
758815	Connectivity issue on port26 because NP6 table configuration has an incorrect member list. Affected models: FG-110xE, FG-220xE, and FG-330xE.
759689	When updated related configurations change, the updated configurations may crash.
760259	On SoC4-based FortiGates (FG-40F, FG-60F, FG-80F, FG-100F) the outbound bandwidth in the bandwidth widget does not adhere to the `outbandwidth` setting.
760661	DDNS interface update status can get stuck if changes to the interface are made rapidly.
761353	Kernel panic occurs on FG-90E after upgrading to 6.4.7.
763185	High CPU usage on platforms with low free memory upon IPS engine initialization.

Bug ID	Description
763739	On FG-200F, the *Outbound* bandwidth in the *Bandwidth* widget does not match the outbandwidth setting.
765452	Slow memory leak in IPS engine 6.091, which persists in 6.107.
766661	Outbandwidth setting does not work in NP7 models when UTM/NTurbo is enabled.
767778	Kernel panic occurs when adding and deleting LAG members on FG-1101E.
770317	FG-5001D backplane interfaces did not work in FG-5913C SLBC system.
771442	Discrepancy between session count and number of active sessions; sessions number creeps high, causing high memory utilization.
777044	On a FortiGate only managed by FortiManager, the FDNSetup Authlist has no FortiManager serial number.
778474	dhcpd is not processing discover messages if they contain a 0 length option, such as 80 (rapid commit). The warning, `length 0 overflows input buffer`, is displayed.
797993	Using outbound traffic shaping and IPS NTurbo together in NP7 platforms causes some traffic to be blocked.

Upgrade

Bug ID	Description
754180	MAC address group is missing in the configuration after upgrading if it has members with other address groups that come behind the current one.
765493	After upgrading to 6.4.7, a web filter profile within flow-based firewall policies appears with a proxy mode feature set.

User & Authentication

Bug ID	Description
556724	LLDP neighbors cannot be seen on virtual switch ports.
682394	FortiGate is unable to verify the CA chain of the FSSO server if the chain is not directly rooted to FSSO endpoint.
691838	Memory leaks and crashes observed during stress long duration performance test when using FortiToken Cloud.
700838	FortiOS does not prompt for token when using RADIUS and two-factor authentication to connect to IPsec IKEv2.

Bug ID	Description
701356	When a GUI administrator certificate, `admin-server-cert`, is provisioned via SCEP, the FortiGate does not automatically offer the newly updated certificate to HTTPS clients. FortiOS 7.0.0 and later does not have this issue.
709964	Apple devices cannot load the FortiAuthenticator captive portal via the system pop-up only.
711263	`diagnose fortitoken-cloud sync` fails when user email address is longer than 35 characters.
725327	FSSO user fails to log in with principal user name.
739702, 741403	There are unknown user logins on the FortiGate and the logs do not have any information for the unknown user.
744014	LLDP neighbors cannot be seen on virtual switch ports.
750551	DST_Root_CA_X3 certificate is expired.
751763	When MAC-based authentication is enabled, multiple RADIUS authentication requests may be sent at the same time. This results in duplicate sessions for the same device.
755302	The fnbamd process spikes to 99% or crashes during RADIUS authentication.
757883	FortiGate blocks expired root CA, even if the cross-signed intermediate CA of the root CA is valid.
765136	Dynamic objects are cleared when there is no connection between the FortiGate and FortiManager with NSX-T.

VM

Bug ID	Description
722290	Azure slow path NetVSC SoftNIC has stuck RX. If using an IPsec tunnel, use UDP/4500 for ESP protocol (instead of IP/50) when SR-IOV is enabled. On the phase 1 interface, use `set nattraversal forced`. UDP/4500 is the fast path for Azure SDN, and IP/50 is the slow path that stresses guest VMs and hypervisors to the extreme. If using cross-site IPsec data backup, use Azure VNet peering technology to build raw connectivity across the site, rather than using the default IP routing based on the assigned global IP address.
736067	NSX connector stops updating addresses sometimes.
739376	vmwd gives an error when folders are created in the vSphere web interface, and vmwd ignores the IP addresses from vApp.
759300	gcpd has signal 11 crash at `gcpd_mime_part_end`.

VoIP

Bug ID	Description
757477	PRACK will cause voipd crashes when the following conditions are met: `block-unknown` is disabled in the SIP profile, the PRACK message contains SDP, and PRACK fails to find any related previous transactions (this is not a usual case).

Web Filter

Bug ID	Description
677234	Unable to block webpages present in the external list when accessing them through the Google Translate URL.
717619	Running a remote CLI script from FortiManager can create a duplicated FortiGuard web filter category.
739349	Web filter local rating configuration check might strip the URL, and the URL filter daemon does not start when `utm-status` is disabled.

WiFi Controller

Bug ID	Description
720497	MAC authentication bypass is not working for some clients.
727301	Unable to quarantine hosts behind FortiAP and FortiSwitch.
733608	FG-5001D is unable to display managed FortiAPs after upgrading.
734801	Some Apple devices cannot handle 303/307 messages, and may loop to load the external portal page and fail to pass authentication. Some Android devices cannot process JavaScript redirect messages after users submit their username and password.
741946	FortiGate is not recognizing attribute 49, Acct-Terminate-Cause Value (6) Admin Reset, from RFC 2866.
748154	802.1X clients are disconnected following a FortiGuard update.
748479	cw_acd is crashing with signal 11 and is causing APs to disconnect/rejoin.
750425	In RADIUS MAC authentication, the FortiGate NAS-IP-Address will revert to `0.0.0.0` after using the FortiGate address.
776239	cw_acd is crashing with `signal 11 (Segmentation fault) received`.

Common Vulnerabilities and Exposures

Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE references
752134	FortiOS 6.4.9 is no longer vulnerable to the following CVE Reference: • CVE-2021-42757
752450	FortiOS 6.4.9 is no longer vulnerable to the following CVE Reference: • CVE-2021-44168

Known issues

The following issues have been identified in version 6.4.9. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Anti Virus

Bug ID	Description
702646	Re-enable JavaScript heuristic detection and fix detection blocking content despite low rating.
752420	If a .TAR.BZ2 or .TAR.GZ archive contains an archive bomb inside its compressed stream, the AV engine will time out.

Application Control

Bug ID	Description
787130	Application control does not block FTP traffic on an explicit proxy.

DNS Filter

Bug ID	Description
692482	DNS filter forwards the DNS status code 1 `FormErr` as status code 2 `ServFail` in cases where the redirect server responses have no question section.

Explicit Proxy

Bug ID	Description
755298	SNI `ssl-exempt` result conflicts with CN `ssl-exempt` result when SNI is an IP.
765761	Firewall with forward proxy and UTM enabled is sending TLS probe with forward proxy IP instead of real server IP.

Bug ID	Description
780211	`diagnose wad stats policy list` output displays information for only 20 proxy policies, so not all policies are included.

Firewall

Bug ID	Description
732604	TCP zero window advertisements not occurring in proxy mode and causing premature server disconnects.
767226	When a policy denies traffic for a VIP and `send-deny-packet` is enabled, the `mappedip` is used for the RST packet's source IP instead of the external IP.
770668	The packet dropped counter is not incremented for `per-ip-shaper` with `max-concurrent-session` as the only criterion and offload disabled on the firewall policy.
773035	Custom services name is not displayed correctly in logs with a port range of more than 3000 ports.
780721	Some firewall policies do not work on FG-2500E after upgrading.

FortiView

Bug ID	Description
683654	FortiView pages with FortiAnalyzer source incorrectly display a *Failed to retrieve data* error on all VDOM views when there is a newly created VDOM that is not yet registered to FortiAnalyzer. The error should only show on the new VDOM view.
692734	When using the *5 minutes* time period, if the FortiGate system time is 40 to 59 second behind the browser time, no data is retrieved.

GUI

Bug ID	Description
440197	On the *System* > *FortiGuard* page, the override FortiGuard server for *AntiVirus & IPS Updates* shows an *Unknown* status, even if the server is working correctly. This is a display issue only; the override feature is working properly.
473841	Newly created deny policy incorrectly has logging disabled and can not be enabled when the CSF is enabled.

Bug ID	Description
602397	Managed FortiSwitch and FortiSwitch *Ports* pages are slow to load when there are many managed FortiSwitches.
630216	A user can browse HA secondary logs in the GUI, but when a user downloads these logs, it is the primary FortiGate logs instead.
653952	*The web page cannot be found* is displayed when a dashboard ID no longer exists. **Workaround**: load another page in the navigation pane. Once loaded, load the original dashboard page (that displayed the error) again.
663558	*Log Details* under *Log & Report* > *Events* displays the wrong IP address when an administrative user logs in to the web console.
688016	GUI interface bandwidth widget does not show correct data for tunnel interface when ASIC offload is enabled on the firewall policy.
695163	When there are a lot of historical logs from FortiAnalyzer, the FortiGate GUI *Forward Traffic* log page can take time to load if there is no specific filter for the time range. **Workaround**: provide a specific time range filter, or use the FortiAnalyzer GUI to view the logs.
713529	When a FortiGate is managed by FortiManager with FortiWLM configured, the HTTPS daemon may crash while processing some FortiWLM API requests. There is no apparent impact on the GUI operation.
734773	On the *System* > *HA* page, when *vCluster* is enabled and the management VDOM is not the root VDOM, the GUI incorrectly displays management VDOM as primary VDOM.
735248	On a mobile phone, the WiFi captive portal may take longer to load when the default firewall authentication login template is used and the user authentication type is set to HTTP. **Workaround**: edit the login template to disable HTTP authentication or remove the href link to googleapis.
739827	On FG-VM64-AZURE, administrator is logged out every few seconds, and the following message appears in the browser: *Some cookies are misusing the recommended "SameSite" attribute*.
743477	On the *Log & Report* > *Forward Traffic* page, filtering by the *Source* or *Destination* column with negation on the IP range does not work.
746953	On the *Network* > *Interfaces* page, users cannot modify the TFTP server setting. A warning with the message *This option may not function correctly. It is already configured using the CLI attribute: tftp-server.* appears beside the *DHCP Options* entry. **Workaround**: use the CLI.
751482	cmbdsvr signal 11 crash occurs when a wildcard FQDN is created with a duplicate ID.
758820	The GUI cannot restore a CLI-encrypted configuration file saved on a TFTP server. There is no issue for unencrypted configuration files or if the file is encrypted in the GUI.
761615	Unable to see details of Apache.Struts.MPV.Input.Validation.Bypass log.
763925	GUI shows user as expired after entering a comment in guest management.
764744	On the *Network* > *Explicit Proxy* page, the GUI does not support configuring multiple outgoing IP addresses.

Bug ID	Description
	Workaround: use the CLI.
787565	When logged in as guest management administrator, the custom image shows as empty on the user information printout. **Workaround**: use the regular *Guest Management* page.

HA

Bug ID	Description
662978	Long lasting sessions are expired on HA secondary device with a 10G interface.
677552	After two quick failovers, VPN does not work until rekey.
683584	The hasync process crashed because the write buffer offset is not validated before using it.
683628	The hasync process crashes often with signal 11 in cases when a CMDB mind map file is deleted and some processes still mind map the old file.
717785	HA primary does not send anti-spam and outbreak prevention license information to the secondary.
750829	In large customer configurations, some functions may time out, which causes an unexpected failover and keeps high cmdbsvr usage for a long time.
751072	HA secondary is consistently unable to synchronize any sessions from the HA primary when the original HA primary returns.
752928	fnbamd uses `ha-mgmt-interface` for certificate related DNS queries when `ha-direct` is enabled.
754599	SCTP sessions are not fully synchronized between nodes in FGSP.
760562	hasync crashes when the size of hasync statistics packets is invalid.
764873	FGSP cluster with UTM does not forward UDP or ICMP packets to the session owner.
765619	HA desynchronizes after user from a read-only administrator group logs in.
766842	Long wait and timeout when upgrading FG- 3000D HA cluster due to vluster2 being enabled.
771389	SNMP community name with one extra character at the end stills matches when HA is enabled.
771999	Sessions not synchronized to HA secondary on an FGSP and FGCP combined setup.
779180	FGSP does not synchronize the `helper-pmap` expectation session.
779512	If the interface name is a number, an error occurs when that number is used as an `hbdev` priority.
782769	Unable to form HA pair when HA encryption is enabled.
785514	In some cases, the fgfmd daemon is blocked by a query to the HA secondary checksum, and it will cause the tunnel between FortiManager and the FortiGate to go down.

Hyperscale

Bug ID	Description
796368	Traffic shaping profile does not seem to have an effect on TCP/UDP traffic in hyperscale.
802369	Large client IP range makes fixed allocation usage relatively limited.

Intrusion Prevention

Bug ID	Description
654307	Wrong direction and banned location by quarantine action for `ICMP.Oversized.Packet` in NGFW policy mode.
699775	Fortinet logo is missing on web filter block page in Chrome.
713508	Low download performance occurs when SSL deep inspection is enabled on aggregate and VLAN interfaces when NTurbo is enabled.
739272	Users cannot visit websites with an explicit web proxy when the FortiGate enters conserve mode with `fail-open` disabled. Block pages appear with the replacement message, *IPS Sensor Triggered!*.

IPsec VPN

Bug ID	Description
749509	IPsec traffic dropped due to anti-replay after HA failover.
773313	FG-40F-3G4G with WWAN DHCP interface set as L2TP client shows drops in WWAN connections and does not get the WWAN IP.
777476	When FGCP and FGSP is configured, but the FGCP cluster is not connected, IKE will ignore the `resync` event to synchronize SA data to the FGSP peer.
781403	IKE is consuming excessive memory.
786409	Tunnel had one-way traffic after iked crashed.

Log & Report

Bug ID	Description
702859	*Outdated report files deleted* system event log keeps being generated.
708890	Traffic log of ZTNA HTTPS proxy and TCP forwarding is missing policy name and FortiClient ID.
726231	The default `logtraffic` setting (UTM) in a security policy unexpectedly generates a traffic log.
753904	The reportd process consumes a high amount of CPU.
764478	Logs are missing on FortiGate Cloud from the FortiGate.
768626	FortiGate does not send WELF (WebTrends Enhanced Log Format) logs.
769300	Traffic denied by security policy (NGFW policy-based mode) is shown as `action="accept"` in the traffic log.
774767	The expected reboot log is missing.
776929	When submitting files for sandbox logging in flow mode, `filetype="unknown"` is displayed for PDF, DOC, JS, RTF, ZIP, and RAR files.

Proxy

Bug ID	Description
604681	WAD process with SoC SSL acceleration enabled consumes more memory usage over time, which may lead to conserve mode. **Workaround**: disable SoC SSL acceleration under the firewall SSL settings.
717995	Proxy mode generates untagged traffic in a virtual wire pair.
747915	Deep inspection of SMTPS and POP3S starts to fail after restoring the configuration file of another device with the same model.
755685	Trend Micro client results in FortiGate illegal parameter SSL alert response because the Trend Micro client sent a ClientHello that includes extra data, which is declined by the FortiGate according to RFC 5246 7.4.1.2.

Routing

Bug ID	Description
717086	External resource local out traffic does not follow the SD-WAN rule and specified egress interface when the `interface-select-method` configuration in `system external-resource` is changed.
724541	One IPv6 BGP neighbor is allowed to be configured with one IPv6 address format and shows a different IPv6 address format.
742648	Health check over shortcut tunnel is dead after `auto-discovery-receiver` is disabled/enabled and VWL crash occurs.

745856	The default SD-WAN route for the LTE wwan interface is not created.
	Workaround: add a random gateway to the wwan member.
	`config system sdwan`
	`  config members`
	`  edit 2`
	`  set interface "wwan"`
	`  set gateway 10.198.58.58`
	`  set priority 100`
	`  next`
	`  end`
	`end`

759752	FortiGate is sending malformed packets causing a BGP IPv6 peering flap when there is a large amount of IPv6 routes, and they cannot fit in one packet.
762258	When policy-based routing uses a PPPoE interface, the policy route order changes after rebooting and when the link is up/down.
771052	The `set next-hop-self-rr6 enable` parameter not effective.
771423	BGP route map community attribute cannot be changed from the GUI when there are two 16-byte concatenated versions.
778392	Kernel panic crash occurs after receiving new IPv6 prefix via BGP.
780210	Changing the interface weight under SD-WAN takes longer to be applied from the GUI than the CLI.

Security Fabric

Bug ID	Description
614691	Slow GUI performance in large Fabric topology with over 50 downstream devices.
690812	FortiGate firewall dynamic address resolution lost when SDN connector updates its cache.

Bug ID	Description
712155	The security rating for *Admin Idle Timeout* incorrectly fails for a FortiAnalyzer with less than 10 minutes.
718469	Wrong timestamp printed in the event log received in email from event triggered from email alert automation stitch.
724071	Log disk usage from user information history daemon is high and can restrict the use for general logging purposes.
764825	When the Security Fabric is enabled, logging is not enabled on deny policies.
765525	The deleted auto-scripts are not sent to FortiManager through the auto-update and cause devices go out of sync.
789820	The csfd process is causing high memory usage on the FortiGate.

SSL VPN

Bug ID	Description
730416	Forward traffic log does not generate logs for HTTP and HTTPS services with SSL VPN web mode.
740378	Windows FortiClient 7.0.1 cannot work with FortiOS 7.0.1 over SSL VPN when the tunnel IP is in the same subnet as one of the outgoing interfaces and NAT is not enabled.
741674	Customer internal website (https://cm***.msc****.com/x***) cannot be rendered in SSL VPN web mode.
745554	Logging in with SSO to FortiAnalyzer with SSL VPN web mode fails.
749857	Web mode and tunnel mode could not reflect the VRF setting, which causes the traffic to not pass through as expected.
756753	FQDN in firewall policy is treated case sensitive, which causes SSL VPN failure when redirecting or accessing a URL that contains capitalized characters.
759664	Renaming the server entry configuration will break the connection between the IdP and FortiGate, which causes the SAML login for SSL VPN to not work as expected.
762685	Punycode is not supported in SSL VPN DNS split tunneling.
767869	SCADA portal will not fully load with SSL VPN web bookmark.
771162	Unable to access SSL VPN bookmark in web mode.
772191	Website is not loading in SSL VPN web mode.
774661	SSL VPN web portal not loading internal webpage.
774831	Comma character (,) is acting as delimiter in authentication session decoding when CN format is `Surname, Name`.
781542	Unable to access internal SSL VPN bookmark in web mode.

Bug ID	Description
783508	After upgrading to 6.4.8, NLA security mode for SSL VPN web portal bookmark does not work.
786179	Cannot reach local application (dat***.btn.co.id) while using SSL VPN web mode.

Switch Controller

Bug ID	Description
774848	Bulk MAC addresses deletions on FortiSwitch is randomly causing all wired clients to disconnect at the same time and reconnect.

System

Bug ID	Description
555616	When NTurbo is enabled, it is unexpectedly provided with the wrong traffic direction information (from server or from client) to decide the destination for the data. This causes the traffic to be sent back to the port where it came from.
602141	The extender daemon crashes on Low Encryption (LENC) FortiGates.
639861	Support FEC (forward error correction) implementations in 10G, 25G, 40G, and 100G interfaces for FG-3400E and FG-3600E.<
648085	Link status on peer device is not down when the admin port is down on the FortiGate.
679059	The ipmc_sensord process is killed multiple times when the CPU or memory usage is high.
685674	FortiGate did not restart after restoring the backup configuration via FortiManager after the following process: disable NPU offloading, change NGFW mode from profile-based to policy-based, retrieve configuration from FortiGate via FortiManager, install the policy package via FortiManager.
705878	Local certificates could not be saved properly, which caused issues such as not being able to properly restore them with configuration files and causing certificates and keys to be mismatched.
716250	Incorrect bandwidth utilization traffic widget for VLAN interface based on LACP interface.
717791	Running `execute restore vmlicense tftp` fails and displays `tftp: bind: Address already in use` message.
724085	Traffic fails over EMAC VLAN interface with parent interface in another VDOM on FG-2600F.
738423	Unable to create a hardware switch with no member.
749613	Unable to save configuration changes and get `failed: No space left on device` error.

Bug ID	Description
750123	FG-100F/101F sensor list shows the following deficiencies: missing PSU reading, degree sign is not readable in some CLI windows, and spelling mistakes.
750171	Legitimate traffic is unable to go through with NP6 `synproxy` enabled.
750533	The cmdbsvr crashes when accessing an invalid `firewall vip` mapped IP that causes traffic to stop traversing the FortiGate.
751044	There was no sensor trap function and related log on SoC4 platforms.
751870	User should be disallowed from sending an alert email from a customized address if the email security compliance check fails.
757478	Kernel panic results in reboot due the size of inner Ethernet header and IP header not being checked properly when the SKB is received by the VXLAN interface.
758490	The value of the `extra-init` parameter under `config system lte-modem` is not passed to the modem after rebooting the device.
764252	On FG-100F, no event is raised for PSU failure and the diagnostic command is not available.
764483	After restoring the VDOM configuration, `Interface <VLAN> not found in the list!` is present for VLANs on the aggregate interface.
771267	Zone transfer with FortiGate as primary DNS server fails if the FortiGate has more than 241 DNS entries.
773702	FortiGate running startup configuration is not saved on flash drive.
778116	Restricted VDOM user is able to access the root VDOM.
800333	DoS offload does not work in 6.4.9 and the npd daemon keeps crashing if the `policy-offload-level` is set to `dos-offload` under `config system npu`. Affected platforms: NP6XLite.
801985	Kernel panic occurs when a virtual switch with VLAN is created, and another port is configured with a trunk.

Upgrade

Bug ID	Description
767808	The `asicdos` option for enabling/disabling NP6XLite DoS offloading is missing after upgrading to 6.4.9. Affected platforms: NP6XLite.

User & Authentication

Bug ID	Description
624167	FortiToken Mobile push notification not working with dynamic WAN IP service provider.
756763	In the email collection captive portal, a user can click *Continue* without selecting the checkbox to accept the terms and disclaimer agreement.
777004	Local users named pop or map do not work as expected when trying to add then as sources in a firewall policy.
778521	SCEP fails to renew if the local certificate name length is between 31 and 35 characters.

VM

Bug ID	Description
596742	Azure SDN connector replicates configuration from primary device to secondary device during configuration restore.
617046	FG-VMX manager not showing all the nodes deployed.
639258	Autoscale GCP health check is not successful (port 8443 HTTPS).
668625	During every FortiGuard UTM update, there is high CPU usage because only one vCPU is available.
721439	Problems occur when switching between HA broadcast heartbeat to unicast heartbeat and vice versa.
750889	DHCP relay fails when VMs on different VLAN interfaces use the same transaction ID.
781879	Flex-VM license activation failed to be applied to FortiGate VM in HA. Standalone mode is OK.
794290	Failed to load FFW-VM; `cw_acd: can not find board mac from interfaces` error displayed in console.

WiFi Controller

Bug ID	Description
662714	The `security-redirect-url` setting is missing when the `portal-type` is `auth-mac`.
677994	Newly discovered and authorized FortiAP will cause HA sync issue. On the HA secondary member, if the WTP profile has a radio in monitor mode, it will be changed to AP mode and unset the band.

Bug ID	Description
757189	On FAP-431 and FAP-831, batches of APs are exhibiting control messages that the maximal retransmission limit was reached.
759344	Tunnel VAP client cannot ping its gateway (inner VLAN support).
783209	After upgrading FortiOS from 6.2 to 6.4, a new `arrp-profile` (`arrp-default`) is added as a static entry. FortiManager cannot install the configuration to a managed FortiGate when trying to purge the `arrp-profile` table. **Workaround**: reboot the FortiGate.
790367	FWF-60F has kernel panic and reboots by itself every few hours.
791761	CAPWAP tunnel traffic over WPA2-Enterprise SSID is dropped when offloading is enabled on FG-1800F.

Built-in IPS engine

Resolved engine issues

Bug ID	Description
644638	Policy with a Tor exit node as the source is not blocking traffic coming from Tor.
683066	IPS engine crashes and consumes high CPU.
691338	Performance issue with download dropping to 0 Kbps and slow website access after firmware upgrade.
698247	IPS engine 6.2.071 has several signal 6 crashes at `ovrd_svr_write_done` on corporate firewall.
713508	Low download performance occurs when SSL deep inspection is enabled on aggregate and VLAN interfaces when nTurbo is enabled.
718503	High memory usage by IPS.
721435	Download breaks when the policy is flow-based with deep inspection, and the NCP application is used on the host.
730235	The IPS engine application crashed during traffic testing (FG-5001E, FG-5001E1).
731459	In NGFW policy mode, disabling a security policy does not stop the current traffic from passing through the firewall.
735893	After the Chrome 92 update, in FOS 6.2, 6.4, or 7.0 running an IPS engine older than version 5.00246, 6.00099, or 7.00034, users are unable to reach specific websites in proxy mode with UTM applied. In flow mode everything works as expected.
736906	The default `np-accel-mode basic` seems to cause sporadic HTTPS deep inspection transaction failures with application control.
738144	The UTM function only works for a few seconds in a GRE session.
741643	Traffic may be incorrectly blocked or match the wrong security policy in NGFW policy mode.
744352	Some websites open very slow in flow mode with SSL deep inspection (5.0245 and 5.0246).
744888	FortiGate drops SERVER HELLO when accessing some TLS 1.3 websites using a flow-based policy with SSL deep inspection.
745163	The ad.doubleclick.net website is not able to open in flow mode with deep packet inspection and a security profile in Chrome.
752466	Deep inspection is causing downloads to fail in an ADVPN environment.
752540	FortiGate keeps outputting warning messages while rebooting.
754216	Flow mode web filter replacement message is not displayed using upstream proxy when using HTTPS.

Bug ID	Description
754579	Application performance is ten times worse when IPS is applied in flow mode.
755223	There is no detection trigger packet in the PCAP.
755294	Firefox gives `SEC_ERROR_REUSED_ISSUER_AND_SERIAL` error when ECDSA CA is configured for deep inspection.
755851	Mixed mode inspection causing SSL error for pass through proxy traffic.
756398	An invalid character string is inserted in the IPS log sent to the TCP syslog server.
756616	High CPU usage in proxy-based policy with deep inspection and IPS sensor.
757122	The wildcard strings do not work as expected.
757314	IPS engine crashes after upgrading to 6.4.7 and is affecting traffic.
757951	CIFS oversize files cannot be blocked.
759194	FortiGate seems to have inserted wrong the timestamp into the PCAP data.
760555	Web filter UTM logged unexpected URLs, such as `url="https:///"`.
765859	Repeated IPS engine signal 11 and signal 7 crashes occur.
774957	Web filter URL static filter is blocking all traffic.
775566	Some websites do not load with flow-based and deep SSL inspection.
777464	The `updated` application crashes after running scripts.
781894	When using a web filter in NGFW mode, websites do not open according to the correct matching policy.
790490	Shared memory is not released and causes the device to enter into conserve mode.
792312	HTTPS traffic cannot pass ESXi FortiGate VM when IPS and deep inspection are enabled.
802465	`ERR_SSL_PROTOCOL_ERROR` occurs when loading a website in flow mode.

Limitations

Citrix XenServer limitations

The following limitations apply to Citrix XenServer installations:

- XenTools installation is not supported.
- FortiGate-VM can be imported or deployed in only the following three formats:
  - XVA (recommended)
  - VHD
  - OVF
- The XVA format comes pre-configured with default configurations for VM name, virtual CPU, memory, and virtual NIC. Other formats will require manual configuration before the first power on process.

Open source XenServer limitations

When using Linux Ubuntu version 11.10, XenServer version 4.1.0, and libvir version 0.9.2, importing issues may arise when using the QCOW2 format and existing HDA issues.